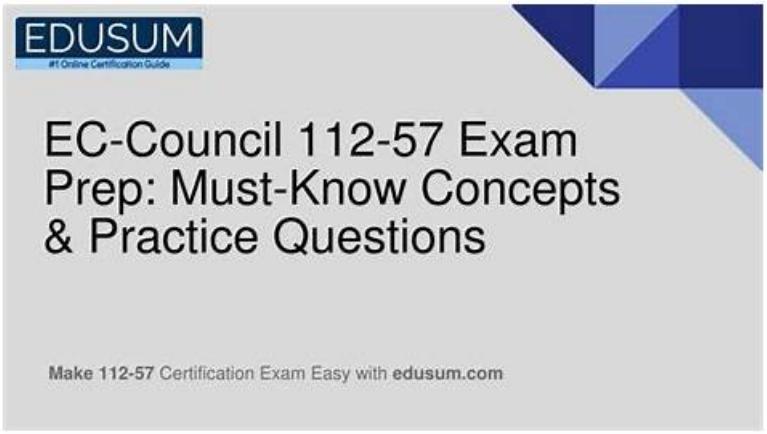
# Three EC-COUNCIL 112-57 Exam Questions Formats - Make Your Exam Preparation Easy




How to get to heaven? Shortcart is only one. Which is using PassTorrent's EC-COUNCIL 112-57 Exam Training materials. This is the advice to every IT candidate, and hope you can reach your dream of paradise.

Our 112-57 study materials are willing to stand by your side and provide attentive service, and to meet the majority of customers, we sincerely recommend our 112-57 practice guide to all customers, for our rich experience and excellent service are more than you can imagine. Here are several advantages of 112-57 training guide for your reference: we have free demos for you to download before payment, and we offer one year free updates of our 112-57 exam questions after payment and so on.

**>> Authentic 112-57 Exam Hub <<**

## EC-COUNCIL 112-57 Mock Exams, Exam 112-57 Tips

Our 112-57 study question is compiled and verified by the first-rate experts in the industry domestically and they are linked closely with the real exam. Our test bank provides all the questions which may appear in the real exam and all the important information about the exam. You can use the practice test software to test whether you have mastered the 112-57 Test Practice materials and the function of stimulating the exam to be familiar with the real exam's pace. So our 112-57 exam questions are real-exam-based and convenient for the clients to prepare for the 112-57 exam.

## EC-COUNCIL 112-57 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • Network Forensics: This module introduces network forensic concepts, including event correlation, analyzing network logs, identifying indicators of compromise, and investigating network traffic. |
| Topic 2 | • Defeating Anti-forensics Techniques: This module discusses anti-forensic methods used to hide or destroy evidence. It also explains techniques investigators use to detect hidden data and recover deleted or protected information. |
| Topic 3 | • Malware Forensics: This module introduces malware investigation techniques, including static and dynamic analysis, and examining system and network behavior to understand malicious activity. |
| Topic 4 | • Computer Forensics Investigation Process: This module explains the phases of the forensic investigation process, including pre-investigation, investigation, and post-investigation. It also covers evidence integrity methods such as hashing and disk imaging. |
| Topic 5 | • Data Acquisition and Duplication: This module focuses on methods for collecting and duplicating digital evidence. It explains acquisition techniques, formats, and procedures used to create forensic images and capture system memory. |

| | |
|---|---|
| Topic 6 | • Computer Forensics Fundamentals: This module introduces the core concepts of computer forensics, including digital evidence, forensic readiness, and the role of investigators. It also explains legal and compliance requirements involved in forensic investigations. |
| Topic 7 | • Dark Web Forensics: This module explains the investigation of dark web activities, including analyzing artifacts related to the Tor browser and identifying dark web usage on systems. |
| Topic 8 | • Understanding Hard Disks and File Systems: This module covers disk structures, types of storage drives, and operating system boot processes. It also explains how investigators analyze file systems and recover deleted data. |
| Topic 9 | • Investigating Web Attacks: This module focuses on analyzing web application attacks through server logs and detecting malicious activities targeting web servers and applications. |
| Topic 10 | • Windows Forensics: This module covers forensic investigation in Windows systems, including analysis of memory, registry data, browser artifacts, and file metadata to identify system and user activities. |
| Topic 11 | • Linux and Mac Forensics: This module explains forensic analysis techniques for Linux and Mac systems. It focuses on analyzing system data, file systems, and memory to recover digital evidence. |

## EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) Sample Questions (Q43-Q48):

**NEW QUESTION # 43**
Which of the following steps in forensic readiness planning provides a backup for future reference and assists in presenting evidence in a court of law?

- A. Creating a process for documenting the procedure
- B. Determining the sources of evidence
- C. Identifying the potential evidence required for an incident
- D. Keeping an incident response team ready to review the incident

**Answer: A**

Explanation:
In forensic readiness planning, the goal is to ensure that when an incident occurs, the organization can collect, preserve, and present digital evidence in a manner that remainsreliable, repeatable, and legally defensible. A key requirement for courtroom acceptance is cleardocumentation-often referred to as proper documentation and chain-of-custody support-showing what actions were taken, by whom, when, using which tools, and under what conditions. Creating a defined process for documenting procedures ensures investigators consistently record acquisition steps, handling methods, hashing/verification results, storage locations, access history, and any changes in evidence possession. This documentation becomes a "backup" in the sense that it preserves institutional memory of the investigation steps, allowing future reviewers (auditors, opposing experts, courts) to reconstruct and validate what occurred even long after the incident.
While identifying potential evidence (B) and determining evidence sources (C) are important readiness tasks, they do not themselves create the structured record needed to defend evidence integrity. Keeping an incident response team ready (D) supports operational response, but does not directly ensure admissibility. Therefore, the step that provides future reference and supports court presentation isCreating a process for documenting the procedure (A).

**NEW QUESTION # 44**
Which of the following Windows system files is created in the system drive after OS installation to support the internal functions and system service dispatch stubs to executive functions?

- A. Ntdll.dll
- B. Win32k.sys
- C. Kernel32.dll
- D. Ntoskrnl.exe

**Answer: A**

Explanation:
Ntdll.dllis the Windows user-mode system library that provides manyinternal NT functions(commonly exposed as "NT Native API" routines such asNt*/Zw*) and, critically, contains thesystem service dispatch stubsused by user-mode code to transition into kernel mode for operating system services. In standard Windows architecture, most user-mode applications call higher-level APIs (for example, Win32 APIs inKernel32.dll), which then ultimately rely onNtdll.dllto perform the final step of invoking the kernel through these system call stubs. This is whyNtdll.dllis a core component loaded into nearly every process and is tightly associated with the boundary between user mode and theexecutivecomponents of the OS.
From a forensics viewpoint, understandingNtdll.dllmatters because it is central to how processes request privileged services, and it is frequently referenced in analyses of process execution, API call chains, and certain user-mode hooking techniques used by malware or anti-forensics tools.
By contrast,Ntoskrnl.exeis the kernel image itself (core kernel/executive),Win32k.sysis a kernel-mode graphics/windowing subsystem component, andKernel32.dllprovides higher-level Win32 APIs rather than the primary system-call stub layer.
Hence,Ntdll.dll (C)is the correct answer.

**NEW QUESTION # 45**
Which of the following MAC forensic data components saves file information and related events using a token with a binary structure?

- A. Kexts
- B. Command-line inputs
- C. Basic Security Module
- D. User account

**Answer: C**

Explanation:
On macOS, theBasic Security Module (BSM)provides the system'saudit framework, which records security- relevant activity such asfile access, process execution, authentication events, privilege changes, and other system calls. A key forensic characteristic of BSM auditing is that events are written asbinary audit records composed of "tokens."Each token represents a structured piece of the event (for example: subject/user identity, process ID, command arguments, path, return value, timestamps), and tokens are assembled into complete audit records. Because these audit logs arebinary and tokenized, they are compact, consistent, and designed for reliable parsing and evidentiary reconstruction-important when building timelines of file- related actions and attributing them to specific users and processes.
The other options do not match the "binary token" description.Command-line inputsmay be stored in shell history files but are plain text and not tokenized binary audit records.User accountartifacts (e.g., directory services, plist files) describe identities and settings, not tokenized event logs.Kexts(kernel extensions) are drivers/modules; while they can affect system behavior, they are not the macOS component that stores file
/event records in a binary token format. Therefore, the correct answer isBasic Security Module (C).

**NEW QUESTION # 46**
Wesley, a professional hacker, deleted a confidential file in a compromised system using the "/bin/rm/" command to deny access to forensic specialists.
Identify the operating system on which Don has performed the file carving act.

- A. Linux
- B. Android
- C. Mac OS
- D. Windows

**Answer: A**

Explanation:
The command path /bin/rm is a hallmark of UNIX/POSIX-style operating systems, where core userland utilities are commonly stored under directories such as /bin, /sbin, and /usr/bin. The utility rm (remove) is the standard UNIX command used to delete directory entries that reference a file's data blocks on disk. This layout and command structure do not match Windows, whichuses different filesystem conventions (drive letters, backslashes, and Windows-native executables) and does not provide /bin/rm as a native path. Android, while Linux-kernel-based, typically exposes shell utilities through environments like /system/bin (and newer

systems may use toybox/busybox variants), not the classic /bin hierarchy expected on general-purpose UNIX systems. Between the remaining options, both Linux and macOS are UNIX-like and can include an rm command; however, in digital forensics training and examination contexts, the explicit reference to /bin/rm is most commonly used to indicate a Linux/UNIX command-line environment on a compromised host.
Therefore, the best single-choice answer from the provided options is Linux (D).

**NEW QUESTION # 47**
In which of the following attacks does an attacker trick high-profile executives such as CEOs, CFOs, politicians, and celebrities to reveal critical corporate and personal information through email or website spoofing?

- A. Identity fraud
- B. Spimming
- C. Whaling
- D. Smishing

**Answer: C**

Explanation:
The scenario describes a targeted social-engineering attack aimed specifically athigh-profile individuals (CEOs, CFOs, politicians, celebrities) and usesemail or website spoofingto deceive them into disclosing sensitive information. In digital forensics and incident response documentation, this is most accurately categorized aswhaling, a specialized form of phishing that focuses on "big targets" (often called "high-value targets" or "VIPs"). Whaling campaigns typically use highly tailored pretexts (e.g., legal subpoenas, board communications, invoice/payment requests, HR or executive directives) and may include spoofed sender domains, look-alike websites, or fraudulent login pages to harvest credentials and confidential corporate data.
Because executives often have access to financial systems, strategic documents, and privileged communications, attackers concentrate effort on realism and personalization, making whaling distinct from broad, generic phishing.
By contrast,smishingis phishing conducted via SMS/text messages,spimmingis spam over instant messaging platforms, andidentity fraudis a broader category involving impersonation/misuse of personal data but does not specifically denote the executive-targeted spoofing technique described. Therefore, the attack type in the question isWhaling (A).

**NEW QUESTION # 48**
.....

Braindumps

- 112-57 Latest Exam Fee □ Reliable 112-57 Real Test □ 112-57 Pass4sure Exam Prep □ Simply search for ▹ 112-57 ◃ for free download on ✔ www.pdfvce.com □✔□ □Exam 112-57 Quick Prep
- Quick and Easiest Way of Getting 112-57 EC-Council Digital Forensics Essentials (DFE) Certification Exam □ Search for 【 112-57 】 on □ www.pass4test.com □ immediately to obtain a free download □112-57 Latest Test Cram
- joshqjlk138783.blogrenanda.com, gerardrwon515419.bloginder.com, donnaghkv993378.blogdal.com, chiaragqol828913.shoutmyblog.com, barryorja968895.blogginaway.com, joshqjlk138783.blogrenanda.com, abelwkxu639526.yourkwikimage.com, anitanoof165088.yomoblog.com, esmeekjrf946992.blogdomago.com, bookmarkprobe.com, Disposable vapes